PrivaFone™

DOCKET FILE COPY ORIGINAL

February 16, 1993

Office of the Secretary
Federal Communications Commission
Washington, DC 20554

Re: ET Docket No. 93-1

These comments with enclosures are in response to your Notice of Proposed Rule Making adopted January 4, 1993 and released January 13, 1993.

We agree that the ability to have privacy for cellular communications is important. However, there are many millions of scanners already out there with more to come - and there are several other ways to eavesdrop that utilize equipment having nothing to do with scanners. Hence these proposed rules will really not solve the eavesdropping problem, and will be very difficult, if not impossible, to be specifically understood and/or enforced.

The answer to the privacy issue is to provide a readily available means for preventing eavesdropping by scanners or other devices. A very efficient, high quality and cost-effective privacy system is now being marketed and sold by our company. The national rollout of our products began in early January, 1993 in the Washington/Baltimore market, and is in the process of expanding in the Mid-Atlantic area, and to the Florida, New York and West Coast areas. Soon these privacy products/systems will be actively marketed throughout America, and they are readily available now to anyone in America who wants cellular privacy. We are seeing a very high degree of interest in and enthusiasm for our rather unique privacy products.

Enclosed for your information and consideration are:

- "Closing Comments" by Bob Grove, the Publisher of "Monitoring Times". This provides an evaluation of Public Law 102-556 and the difficulty of enforcing it.
- An article from the "Legal Times" by James J. Harrison, Jr. which explains the eavesdropping problem and how cellular calls should be privatized/protected

1122 Kenilworth Drive • Suite 217 • Baltimore, Maryland 21204 • (410) 494-0144 • FAX (410) 296-8309

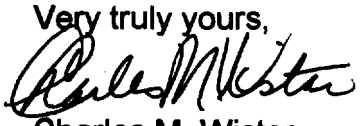
Office of the Secretary
Federal Communications Commission
February 15, 1993

- A brochure from PrivaFone explaining how our cellular privacy products work

In summary we feel that the new law and the proposed rules will not solve the privacy problem, but the PrivaFone system will efficiently and effectively do so. Accordingly, the law and/or the proposed rules should be revised, simplified, and/or possibly eliminated to reflect that efficient solutions to the cellular privacy problems do exist and are readily available to those who want privacy protection.

We would be happy to meet with you at your convenience at any time to answer any questions you may have, and to provide you additional relevant information.

Very truly yours,



Charles M. Wistar
President and CEO

CMW/mab

Enclosure

Another Win for the Cellular Pac

The well-funded Washington lobby known as the Cellular Telecommunications Industry Association (CTIA) once again sneaked a last-minute, self-serving provision into a pending bill just before Congressional adjournment. And once again, it worked.

The profit-driven cellular investors are unconcerned with the erosion of our historical freedom of access to the airwaves which their commercial legislation has wrought; neighboring Canada and even former Communist countries now have more listening rights than Americans.

HR-6191, the "Pay-Per-Call" Bill, became Public Law P.L.102-556 when signed on October 28, 1992, by President Bush. While the major thrust of the Bill is to protect consumers from abusive 900-exchange pay-per-call advertising, it also contains a ringer: an anti-cellular scanner provision.

The issue is not an individual's right to privacy; it is cellular's continuous evasion of their moral and legal responsibility to protect their customers' conversations from being broadcast in the clear. And they have successfully evaded it once again through misleading lobbying, all to avoid paying slightly more for telephone scrambling.

The new law will require the FCC to deny certification after April 28, 1993, to any scanning receiver capable of tuning cellular frequencies, or readily alterable to receive cellular frequencies, or containing a descrambler for digitized cellular calls. Six months later no such scanner can be manufactured or imported.

FCC officials privately admit that they are facing a regulatory nightmare. The current definition of a "scanning receiver" is entirely inadequate to accommodate the new law. And what constitutes "readily altered"? A Notice of Proposed Rulemaking is being prepared and released at this time; a public comment period will follow.

Current cellular-capable scanners should be legally available for at least a year since there is no prohibition against selling them if they were manufactured prior to the cutoff date. Of course, enterprising investors may buy up all the cellular-capable scanners, then scalp the market when other sources dry up!

Scanner owners will still be allowed to modify their own radios, add external converters, buy cellular-capable non-scanning receivers and video equipment, acquire previously-manufactured equipment, purchase government and military equipment as well as test equipment excluded under the provision, repair older scanners indefinitely, and so on.

While the Bill's sponsors assured their colleagues that the proposal would enforce the Electronic Communications Privacy Act of 1986, the wording was contrived to protect cellular interests only—no reference is made in the new law to the other services covered under the ECPA.

The new law is welcome news to drug dealers who use cellular telephones as a tool of the trade. Their criminal activities are commonly reported to law enforcement authorities by conscientious listeners who happen to overhear deals going down, reporting drop points and contacts. The criminals will now be protected.

Perhaps there is some light at the end of the tunnel; President-Elect Bill Clinton has promised to re-examine such politically-inspired bills signed into law by the outgoing administration for possible reversal.

Perhaps the new administration will be perceptive enough to reverse both P.L.102-556 and the ill-worded and commercially-inspired ECPA '86, reverting to the wisdom of section 605 of the 1934 Communications Act; this section acknowledges that Americans may overhear conversations not intended for them, but provides stiff penalties for those who misuse that information. This is good law.

Bob Grove
Publisher

SPECIAL REPORT

LAW OFFICE TECHNOLOGY

Cellular Phones Are Weakest Security Link

BY JAMES J. HARRISON JR.

Your day begins with a quick call from your car phone to a client.

"I found a key weakness in the defendant's position that appears to be critical to his defense," you say, quickly outlining how you plan to take advantage of that weakness.

Fast forward several weeks to the trial. After presenting your client's case, you sit down with a smile on your face, believing you will undoubtedly win.

But wait! What's happening? It seems as if the opposing counsel already knew how you planned to expose his client's weakness and he quickly tears your argument to pieces. How could that be? You haven't discussed it with anyone.

Or have you? That cellular phone conversation you had several weeks ago was being monitored. In fact, it was sent over the airwaves to anyone who happened to be tuned in to a scanner or other eavesdropping equipment.

Today there are more than 10 million scanners on the street that

SEE CELLULAR PHONE, PAGE 32

Intelligent Systems Form the Cutting Edge

BY PAUL C. KAINEN

By now it has become clear that new technology—computerization and networking—is changing both the way that lawyers and lobbyists work and the very nature of the issues facing them. The cutting edge of that new technology is intelligent systems.

What is an intelligent system? This is really two questions. A system is a collection of hardware and software designed to serve a group of people within some specific social or organizational context. For instance, Lexis is a system to provide lawyers with improved access to case law.

A system is intelligent to the extent it anticipates the needs and capabilities of its users in order to offer better service. For example, if a single inadvertent keystroke can abruptly terminate an online information search, dumping irretrievably all the work accomplished, then the search system certainly does not qualify as intelligent. Furthermore, if the screen display is not easy to understand or if the delay in getting information is so long that the

SEE INTELLIGENT SYSTEMS, PAGE 28

LAW OFFICE TECHNOLOGY

Cellular Phones Are Easy to Monitor and Hard to Secure

CELLULAR PHONE FROM PAGE 27

can easily monitor cellular telephone conversations. Available for as little as $150, these hand-held units can easily be programmed to search for conversations.

The Weak Links

Although many eavesdroppers are hobbyists tuning in to police and fire dispatchers and to the occasional juicy cellular conversation, others have joined an underground industry of eavesdroppers who use sophisticated technology to garner intelligence of value to a litigant, business competitor, or political foe.

While many firms spend thousands of dollars securing their high-tech data centers from espionage, they often ignore the less obvious, low-tech links in their networks. Cellular phones are extremely vulnerable and are often the weakest link in a company's communications network.

What is surprising to many attorneys is how easy it is to monitor cellular-telephone conversations. An eavesdropper can purchase a scanner from an electronics store, program the equipment to a band of cellular-phone frequencies, and immediately begin tuning in to conversations. Sophisticated scanner users purchase special devices that can be aimed directly at your car to determine what frequency your call will use. Once they aim, they can just tune in and record your conversations.

In at least two Canadian provinces, some eavesdroppers have even gone commercial. In the same spirit of those who attempt to photograph celebrities off guard, scanner buffs spend their days recording conversations. When a conversation of potential value is captured, an offer to sell the information can be made to a competitor, the media, or whomever the Listening Tom thinks might pay for its contents.

Although many eavesdroppers are hobbyists tuning in to police and fire dispatchers, others have joined an underground industry of eavesdroppers who use sophisticated technology to garner intelligence of value to a litigant, business competitor, or political foe.

Even something as basic as calling in to retrieve voice-mail messages is risky. In today's world of "telephone tag," many clients leave detailed messages on voice mail systems to save time. Yet when the unsuspecting lawyer calls in from a car phone to retrieve messages, every word can be picked up by the eavesdropper. In the United States, the Electronic Communications Privacy Act of 1986 makes it illegal to monitor, tape, or distribute the content of most electronic, wire, or private oral communications. Yet this law is virtually impossible to enforce.

Most scanners purchased today include a warning stating that it is illegal to listen to certain frequencies. But that is like telling a television buff not to watch certain channels.

To stop would-be eavesdroppers and prevent critical information from being overheard, you can exercise a number of management and technological options to safeguard yourself from "spies."

Management Solutions

As a first step, management should warn firm members about the inherent risks in using cellular phones. Basic points to remember:

- Use your cellular phone only for short conversations that contain no privileged information.
- Save important client information for land-line phones. Never divulge such information as names, accounts, or telephone numbers.
- Be wary that the called party may not realize the security risks involved and may begin to discuss sensitive information. Warn your caller up front that you are talking from a cellular phone and to keep the conversation simple and to the point.
- Watch what you say and talk in generalities. Don't state, "I'm reviewing John Smith's divorce case and have found a loophole in the prenuptial agreement." Instead, say, "I'm reviewing our case and we need to schedule a meeting."

Even the most security-minded firms have difficulty warning their employees about the hazards of cellular phones. It is very difficult to monitor all employee calls, and many attorneys, while striving to utilize valuable billable time, often forget the inherent risks.

In addition, the very reason that firms purchase cellular phones is questionable since associates cannot freely discuss business while on the road.

Technological Solutions

To meet growing concerns, a number of options are now available for consumers to use with the current cellular system.

All of the current high-tech solutions operate as scrambling devices, basically working like paper shredders. When a phone call is placed, the scrambling equipment takes the sound of the caller's voice and "rips" it into millions of pieces for transmission over the airwaves. The result—a high-pitched garbled sound. The

SEE CELLULAR PHONE, PAGE 33

LAW OFFICE TECHNOLOGY

CELLULAR PHONE FROM PAGE 32

eavesdropper is off on a search for an unprotected conversation.

Many of these existing solutions work by requiring callers on both ends of a conversation to have a descrambling device to unscramble the message. That works well when someone is calling into the office for messages or to talk with colleagues.

Another device builds on that approach by funneling calls from cellular phones through the person's office or home telephone. The patented device means that only one party on the line needs to have a scrambler. The scrambling device is plugged into the cellular telephone handset; a second piece of equipment is connected to the central telephone line, usually in the customer's office. Simply place a call to your base station or office, and after automatically being rolled onto a land line, dial anyone, anywhere in the world. All land-line calls are private.

More expensive end-to-end encryption options—considered the ultimate in security—are available. One of the more popular units is the STU-III (Secure Telephone Unit). Models manufactured by Motorola begin at $5,000, and each phone must have attached to it a $2,000 to $3,000 unit.

One kind of scrambling device works by plugging into the cellular telephone handset. Then a second piece of equipment is connected to the central telephone line, usually in the customer's office. Simply place a call to your office, and after automatically being rolled onto a land line, dial anyone, anywhere in the world.

When choosing a high-tech solution for your office, consider the following:

- Find a convenient and easy-to-use system. You don't want to invest in a product that is cumbersome because your employees simply won't use it.
- Select a system that works no matter where you travel. What's the purpose if you're on business in another state and cannot use your car phone?
- Opt for a product that is easy to install.

Managers must remember that cellular telephones are just as vulnerable to espionage as the high-tech computer centers they take pains to secure.

Only by understanding where leaks may exist and developing a comprehensive program to plug them, can management prevent sensitive data from getting into the wrong hands.

James J. Harrison Jr., formerly vice president, general counsel, and chief financial officer of McCormick and Co., currently is vice president of finance and administration for the PrivaFone Corp., which specializes in privatizing cellular communications.

Because It's Nobody's Business But Your Own.

With a PrivaFone system, your conversation is safe-guarded and secure to any phone in the world. No matter what you discuss on your cellular phone – business strategies, financial issues, personal matters – PrivaFone locks in the line so the only one listening is the person you called. This system gives you the freedom to call anyone, anywhere, at any time because the called party doesn't need any special equipment.

Show clients and customers that you're serious about confidentiality. When your associates realize you've provided them with a secure channel of communications, it not only makes them more comfortable doing business with you, but PrivaFone will provide the kind of safe environment that is conducive to talking, without the worry or the inconvenience of having to pull over to a pay phone or other landline to finish a conversation. After all, what good is a car phone if you can't use it?

Owning A PrivaFone Pays Off In More Than Complete Call Security.

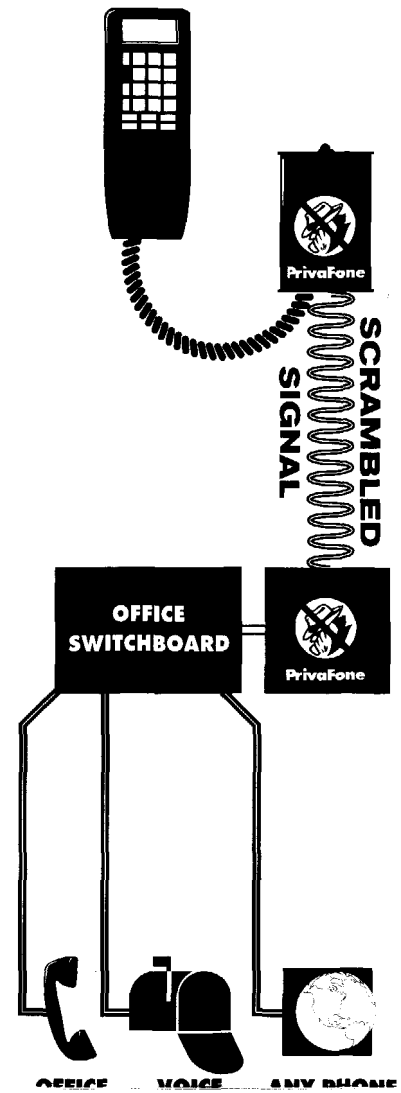
Voicemail, the phone in your hotel room, your home, or even at your desk, can be protected with one of the PrivaFone System components. Make or receive direct PrivaFone calls to or from any landline or cellular phone in the world equipped with PrivaFone, or indirectly through your company's PrivaFone-equipped switchboard.

PrivaFone plugs right into most popular models of cellular phone. You can take it with you even if you purchase a new phone or switch cellular companies. Companion units interface transparently with all standard phone lines.

To order, for more information on the new standard in business communication privacy, or for the dealer nearest you, call us at 1-800-FOR-PRIV(acy).

Because It's Nobody's Business But Your Own!

How PrivaFone Works



Call your office from your PrivaFone-equipped cellular phone.

The PrivaFone Line Privacy Unit at your switchboard completes the scrambled call and then you can be directed to any extension or voicemail.

Most importantly, the PrivaFone call can be connected by most switchboards to an outside line, and then you may dial any phone in the world.

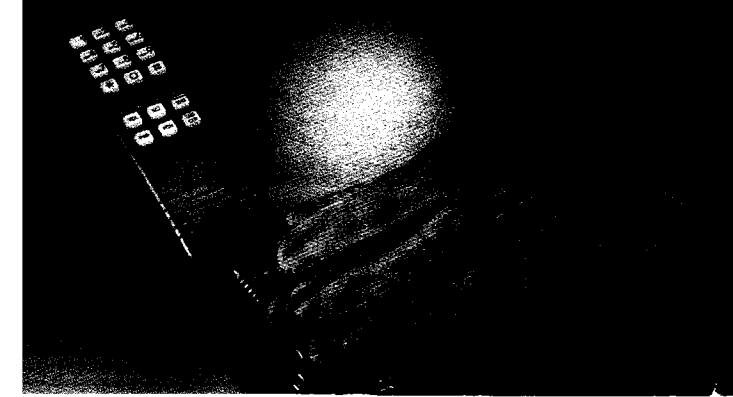
Or, The PrivaFone Call Extender can do the switching if your switchboard can't.

In each case, you can speak with the comfort that comes from knowing that the cellular portion of the call is always scrambled.

YOUR CAR PHONE

The calls you make on your cellular phone may not be as private as you think. Every time you call, the signal is broadcast through the airwaves where it could be intercepted by anyone with a *scanner* within a *range* of up to *50 miles*. And if you think no one is listening, then consider that over *10 million scanners* have been sold in the U.S. alone.

PrivaFone™ is the personal phone security system that *ensures* that your private calls stay private. This patented scrambling system gives you the permanent solution to the problem of compromised cellular security with a convenient state-of-the-art module small enough to fit in your pocket.



PrivaFone™

Because It's Nobody's Business But Your Own.

1122 Kenilworth Drive
Suite 217
Baltimore, MD 21204
410-494-0144
FAX 410-296-8309

Technology By Cycomm Corporation

NOW

ANYONE CAN BREAK

INTO YOUR

PRIVATE OFFICE

WITH THIS

ONE SIMPLE TOOL.